

# Keeping Children Safe Online

## January 2008 - Cyber Security Tip ST05-002

Children present unique security risks when they use a computer—not only do you have to keep them safe, you have to protect the data on your computer. By taking some simple steps, you can dramatically reduce the threats.





### **What unique risks are associated with children?**

When a child is using your computer, normal safeguards and security practices may not be sufficient. Children present additional challenges because of their natural characteristics: innocence, curiosity, desire for independence, and fear of punishment. You need to consider these characteristics when determining how to protect your data and the child.

You may think that because the child is only playing a game, or researching a term paper, or typing a homework assignment, he or she can't cause any harm. But what if, when saving her paper, the child deletes a necessary program file? Or what if she unintentionally visits a malicious web page that infects your computer with a virus? These are just two possible scenarios. Mistakes happen, but the child may not realize what she's done or may not tell you what happened because she's afraid of getting punished.

Online predators present another significant threat, particularly to children. Because the nature of the internet is so anonymous, it is easy for people to misrepresent themselves and manipulate or trick other users (see [Avoiding Social Engineering and Phishing Attacks](#) for some examples). Adults often fall victim to these ploys, and children, who are usually much more open and trusting, are even easier targets. The threat is even greater if a child has access to email or instant messaging programs, visits chat rooms, and/or uses social networking sites (see [Using Instant Messaging and Chat Rooms Safely](#) and [Staying Safe on Social Network Sites](#) for more information).

### **What can you do?**

-  Be involved - Consider activities you can work on together, whether it be playing a game, researching a topic you had been talking about (e.g., family vacation spots, a particular hobby, a historical figure), or putting together a family newsletter. This will allow you to supervise your child's online activities while teaching her good computer habits.
-  Keep your computer in an open area - If your computer is in a high-traffic area, you will be able to easily monitor the computer activity. Not only does this accessibility deter a child from doing something she knows she's not allowed to do, it also gives you the opportunity to intervene if you notice a behavior that could have negative consequences.
-  Set rules and warn about dangers - Make sure your child knows the boundaries of what she is allowed to do on the computer. These boundaries should be appropriate for the child's age, knowledge, and maturity, but they may include rules about how long she is allowed to be on the computer, what sites she is allowed to visit, what software programs she can use, and what tasks or activities she is allowed to do. You should also talk to children about the dangers of the internet so that they recognize suspicious behavior or activity. The goal isn't to scare them; it's to make them more aware.
-  Monitor computer activity - Be aware of what your child is doing on the computer, including which web sites she is visiting. If she is using email, instant messaging, or chat rooms, try to get a sense of who she is corresponding with and whether she actually knows them.

- ✚ Keep lines of communication open - Let your child know that she can approach you with any questions or concerns about behaviors or problems she may have encountered on the computer.
- ✚ Consider partitioning your computer into separate accounts – Most operating systems (including Windows XP, Mac OS X, and Linux) give you the option of creating a different user account for each user. If you're worried that your child may accidentally access, modify, and/or delete your files, you can give her a separate account and decrease the amount of access and number of privileges she has. If you don't have separate accounts, you need to be especially careful about your security settings. In addition to limiting functionality within your browser (see Evaluating Your Web Browser's Security Settings for more information), avoid letting your browser remember passwords and other personal information (see Browsing Safely: Understanding Active Content and Cookies). Also, it is always important to keep your virus definitions up to date (see Understanding Anti-Virus Software).
- ✚ Consider implementing parental controls - You may be able to set some parental controls within your browser. For example, Internet Explorer allows you to restrict or allow certain web sites to be viewed on your computer, and you can protect these settings with a password. To find those options, click Tools on your menu bar, select Internet Options..., choose the Content tab, and click the Enable... button under Content Advisor. There are other resources you can use to control and/or monitor your child's online activity. Some ISPs offer services designed to protect children online. Contact your ISP to see if any of these services are available. There are also special software programs you can install on your computer. Different programs offer different features and capabilities, so you can find one that best suits your needs. The following web sites offer lists of software, as well as other useful information about protecting children online:
- ✚ GetNetWise - <http://kids.getnetwise.org/> - Click Tools for Families to reach a page that allows you to search for software based on characteristics like what the tool does and what operating system you have on your computer.
- ✚ Yahoooligans! Parents' Guide - <http://yahooligans.yahoo.com/parents/> - Click Blocking and Filtering under Related Websites on the left sidebar to reach a list of software.